



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/765,108	01/16/2001	Alexander Medvinsky	D02538	8249
43471	7590	07/09/2009	EXAMINER	
Motorola, Inc. Law Department 1303 East Algonquin Road 3rd Floor Schaumburg, IL 60196				COLIN, CARL G
ART UNIT		PAPER NUMBER		
2433				
			NOTIFICATION DATE	DELIVERY MODE
			07/09/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing.US@motorola.com

Office Action Summary	Application No.	Applicant(s)	
	09/765,108	MEDVINSKY, ALEXANDER	
	Examiner	Art Unit	
	CARL COLIN	2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 03 April 2009.
 2a) This action is **FINAL**. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-6, 10-12 and 17-23 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) 6 and 10-12 is/are allowed.
 6) Claim(s) 1,3-5,17-19 and 21-23 is/are rejected.
 7) Claim(s) 2 and 20 is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____ .
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)	5) <input type="checkbox"/> Notice of Informal Patent Application
Paper No(s)/Mail Date _____.	6) <input type="checkbox"/> Other: _____ .

DETAILED ACTION

Response to Arguments

1. In communications filed on 4/3/2009, applicant amends claims 6 and 17; cancels claims 7 and 13-16; the following claims 1-6, 10-12, and 17-23 are pending and are presented for examination.
2. Applicant's remarks, filed on 4/3/2009, pages 9-17 with respect to the rejection of claims 1-7 and 10-23 have been considered but they are not persuasive.

Applicant argues that neither Long nor Dent discloses generating a second key stream when a component used to transmit the Real Time Protocol voice packets changes during the communication session as recited in claim 1. Examiner respectfully disagrees. Dent teaches producing new keystream bits (generating new key) when there is handoff (the handoff is due to a change of a component in transmitting the voice packets, see column 3, lines 30-59 and column 4, lines 26-55) that meets the recitation of when a component used to transmit the Real Time Protocol voice packets changes, generate a second key (see column 6, lines 41-58 and column 15, lines 30-44). With respect to applicant's arguments that Long teaches away from Dent, Examiner respectfully disagrees. The prior art mere disclosure of conventional art does not constitute a teaching away because such disclosure does not discredit the conventional art but rather offers a balance depending on design choices (see column 1, lines 42-48). Dent suggests keeping traffic interruption to a minimum (see column 15, lines 20-25). With regard to claims 6 and 13, (see page 9) applicant implies that claim 6 recites the same limitations as claim 1,

Examiner asserts that a change in communication parameter does not equate when a component used to transmit the Real Time Protocol voice packets changes. Examiner respectfully disagrees with applicant's arguments as Long discloses generating a second key stream when the counter reaches the specified value, the change in values meets the recitation of a change in communication parameter (see column 4, lines 5-35; column 2, lines 47-63). In addition, Long discloses generating a second key stream according to a key ID that also meets the recitation of a change in communication parameter (see column 3, lines 19-29). Applicant has not shown how a change in communication parameter is patentably distinct from Long's disclosure. Without conceding to applicant's argument, claims 6 and 13 are also rejected on the same rationale as claim 1 in order to expedite the prosecution. With regards to claim 19, claim 19 recites means plus function and the structures are disclosed in the combined references. Applicant has not shown claim 19 is patentably distinct from the combined references. With respect to claim 17, the claim merely states generating a second key in response to collision detection, Dent discloses a collision is detected wherein the multimedia terminal adapters have the same source identifier (see column 14, lines 21-49) and further discloses generating a second steam in response to handoff as discussed above with respect to claim 1 (see also column 15, lines 30-44). Dent illustrates detecting a collision and restarting a new session (see column 12, line 23 through column 13, line 16, the failure of synchronization is due to a collision as understood by Examiner). Upon further consideration, a new ground of rejection is made in view of Fruehauf et al in combination with the previously cited art.

Specification

3. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: a component used to transmit the Real Time Protocol voice packets changes during the communication session does not have any antecedent basis in the citations provided by applicant (see appeal brief, page 2). A codec is not described in the specification as a component used to transmit the Real Time Protocol voice packets. On the other hand, the passage cited by applicant states,

“MTA 104 receives the packets with the new CODEC with the new set of keys and may optionally keep the old keys for a short period to receive packets that are still using the old CODEC.” (see page 10, lines 13-15).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject

matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-3, 6-7, 10-16, and 19-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,940,508 to **Long et al** in view of US Patent Publication 2002/0006202 to **Fruehauf et al** in view of US Patent 5,081,679 to **Dent**.

As per claim 1, Long et al substantially discloses a system for securely transmitting Real Time Protocol voice packets during a communication session with a remote multimedia terminal adapter over an Internet protocol network; the system comprising: **Long et al** discloses a crypto equipment 10 for receiving the voice packets (see column 2, lines 4-6) the voice packets having a clock counter to synchronize cryptographic operations between encryption equipments 10 and 20 (column 3, lines 19-23) that meets the recitation of *a local multimedia terminal adapter* (crypto equipment 10) *receiving the voice packets having a timestamp* (Clk Counter 30) as a *synchronization source to synchronize cryptographic operations between said local multimedia terminal adapter* (crypto equipment 10) *and said remote multimedia terminal adapter* (crypto equipment 20), *the local multimedia terminal adapter* (crypto equipment 10) comprising, *a local key stream generator* (key generator 80) *for generating a first key stream*; **Long et al** discloses an encryptor equipment is operable to encrypt the data using key generated by the key generator (see column 2, lines 4-6; column 2, lines 16-21 and fig.2; see also column 4, lines 53-56) that meets the recitation of *a packet encryptor that encrypts the voice packets using at least a portion of the first key stream to form encrypted voice packets*. **Long et al** discloses equipments 10 and

20 are similar and for simplicity only one direction will be discussed (i.e. the approach for decryption and equipment 20 is implicit or inherent) and further discloses *the remote multimedia terminal adapter* (equipment 20) *receiving the encrypted voice packets* (see column 2, lines 6-15 and fig. 2), *the remote multimedia terminal adapter further comprising a remote key stream generator* (key generator 80) *for generating the first key stream in order to decrypt the encrypted voice packets* (see column 1, lines 16-18 and column 2, lines 6-8); decryptor equipment is operable to decrypt the data using key generated (see column 2, lines 6-8; column 2, lines 16-21 and fig. 2; see also column 4, lines 53-56) that meets the recitation of *a packet decryptor decrypting the encrypted voice packets using the first key stream*. **Long et al** discloses a rekeying process wherein both key generators generate a second key when equipment 10 performs a switchover during the communication session and both equipments 10 and 20 use the second key stream (see column 2, lines 47-63 and column 4, lines 12-23). **Long et al** is silent about generating a second key stream when a component used to transmit the Real Time Protocol voice packets changes during the communication session. **Fruehauf et al** in an analogous art discloses eliminating loss of data resulting from out-of-sync key changes (see paragraph 41). **Fruehauf et al** discloses encryptor/decryptors that are used for data transfers (see paragraph 36) and further discloses when a transition from one data decryptor to another data decryptor occurs, the data decryptors have changed keys (see paragraph 42) that meets the recitation of *when a component used to transmit the Real Time Protocol voice packets changes during the communication session wherein both key stream generators generate a second key stream*. **Fruehauf et al** discloses both packet encryptors and decryptors use the second key stream (see paragraph 11). Therefore, it would have been obvious to one of ordinary skill in the

art at the time the invention was made to modify **Long et al** to generate a second key stream when a component used to transmit the Real Time Protocol voice packets changes during the communication session because it would eliminate interruptions or loss of data resulting from out-of-sync key changes, delays in the communication media, or loss of data packets that may be in transit during a key transition boundary as suggested by **Fruehauf et al** (see paragraph 41).

Long et al is silent about the data being voice data. It is apparent one of ordinary skill in the art that the invention may be applied to any type of data communication as known in the art including radio communication using voice packets. **Dent** in an analogous art also discloses synchronization using real-time clock and counters operable to synchronize cryptographic operations between a transmitter and a receiver in cellular radio system using voice packets (see column 12, lines 23-51). The equipment may be used for secure communication over digital channel for converting a voice signal into digital signal (see column 8, lines 54-66). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the system of **Long et al** into cellular radio communications so as to securely transmit voice packets using synchronization technique and convert voice packet to digital data stream and vice versa as suggested by **Dent** above.

As per claim 3, the references as combined above disclose the limitation of wherein the second key stream is generated when a Message Authentication Code algorithm change occurs, for example (see **Long et al**, column 3, lines 19-23) (see also **Dent**, column 10, lines 14-25).

As per claim 21, Long et al discloses the limitation of providing key derivation or a pseudorandom function based on a counter, a known value, and key variable, for example (see column 3, lines 5-23) that meets the recitation of wherein the second key stream is generated by re-executing the following key derivation function: $F(S, \text{"End-End RTP Key Change } <N>\text{"})$ where N is a counter incremented whenever a new set of Real Time Protocol keys is re-derived for the same media stream session; $F(\)$ is a one-way pseudo-random function used for the purpose of key derivation; S is a shared secret which includes a random value shared between the two endpoints and is known only to those two endpoints or a trusted server, and "End-End RTP Key Change $<N>$ " is a label that is used as a parameter to the key derivation function $F()$, $<N>$ stands for an ASCII representation of a decimal number, representing a counter. Similar algorithm in the claimed invention of f as a function of a secret key and a parameter can be found in cryptography textbook known in the art. (See also **Dent**, column 15, lines 20-50).

Claim 22 is similar to the rejected **claim 21** except for adding a synchronization source identifier, which is known in the art as found in US patents 6,2754,71 and 6,122,665. **Long et al** also uses a key identifier that meets the recitation of synchronization source identifier, for example (see **Long et al**, column 3, lines 5-23). Therefore, **claim 22** is rejected on the same rationale as the rejection as the rejection of **claim 21**.

As per claim 19, claim 19 recites similar limitations as claim 1 except for using a means plus function. **Long et al** substantially discloses a system for securely transmitting voice packets

during a communication session from a local location to a remote location over an Internet protocol network; the system comprising: *a local key stream generator* (key generator 80, fig. 2) that means the recitation of *a means for generating a first key stream at the local location*; an encryptor equipment that means the recitation of *a means for encrypting the voice packets using at least a portion of the first key stream to form encrypted voice packets* (see column 2, lines 4-6; column 2, lines 16-21 and fig.2; see also column 4, lines 53-56); *a means forwarding voice packets encrypted with the second Real Time Protocol key stream to the remote location* (see column 3, lines 19-24 and column 4, lines 47-49); *a means for generating the first key stream at the remote location for encrypting the voice packets* (key generator 80 in equipment 20, fig. 2), and decryptor equipment is operable to decrypt the data using key generated (see column 2, lines 6-8; column 2, lines 16-21 and fig. 2; see also column 4, lines 53-56) that meets the recitation of *a means for decrypting the encrypted voice packets using the first key stream*. **Long et al** discloses a rekeying process wherein both key generators generate a second key when equipment 10 performs a switchover during the communication session and both equipments 10 and 20 use the second key stream (see column 2, lines 47-63 and column 4, lines 12-23) that meets the recitation of *wherein both means for generating are capable of generating a second key stream when a component used to transmit the Real Time Protocol voice packets changes during the communication session*, **Long et al** also discloses the voice packets having a clock counter to synchronize cryptographic operations between encryption equipments 10 and 20 (column 3, lines 19-23) that meets the recitation of *wherein the voice packets having a timestamp as a synchronization source operable to synchronize cryptographic operations between said local and remote locations*.

Claim 19 is also rejected on the same rationale as the rejection of claim 1 above.

As per claim 23, the references as combined above disclose the limitation of further comprising a means for synchronizing the voice packets, for example (see **Dent**, column 12, lines 23-51).

5. **Claims 4 and 5** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 5,940,508 to **Long et al** in view of US Patent 5,081,679 to **Dent** in view of US Patent Publication 2002/0006202 to **Fruehauf et al** as applied to claim 1 above and further in view of US Patent Publication US 2002/0031126 to **Crichton et al** and Non-Patent Literature “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”, May 2000; **RFC 2833**.

As per claims 4 and 5, Long et al substantially teaches forwarding/receiving encrypted packets from a local to a remote end, for example (see column 2, lines 4-8). Although **Long et al** is silent about a gateway controller, which is well known in the art of Internet Protocol network for connecting different protocol networks, if it is interpreted as software, the disclosure of **Long et al** meets the claimed limitation. **Crichton et al.** in an analogous art teaches a system for bit synchronous network communications over packet networks including Internet protocol network using gateways in an end-to-end communication path to perform analog to digital conversion and to communicate with packet network in a manner known in the art, for example

(see page 5, paragraphs 0042 and 0047; see also background). The use of gateway is also explicitly cited in RFC 2833 for forwarding encrypted data. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to provide a gateway controller as taught by **Crichton et al** or in RFC 2833 (page 1) for forwarding and receiving encrypted packets through an Internet protocol to perform analog to digital conversion and to communicate with packet network in a manner known in the art. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Crichton et al.** so as to perform analog to digital conversion and to communicate with packet network in a manner known in the art.

6. **Claims 17 and 18** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,940,508 to **Long et al** in view of US Patent 5,081,679 to **Dent** in view of US Patent Publication US 2002/0031126 to **Crichton et al.**

As per claim 17, Long et al substantially discloses a method comprising *generating a first Real Time Protocol key stream for encrypting the voice packets* (see column 4, lines 53-56), *forwarding encrypted voice packets to the remote location* (see column 2, lines 4-8; column 2, lines 16-21 and fig.2; see also column 4, lines 53-56). **Long et al** discloses a rekeying process wherein the key generator in equipment 10 generates a second key for encrypting the voice packets in response to any loss of data synchronization or need to provide data re-synchronization (see column 2, line 63 through column 3, line 5). **Long et al** also discloses

wherein the multimedia terminal adapters have the same source identifier (see column 3, lines 24-29); **Long et al** further discloses *forwarding voice packets encrypted with the second Real Time Protocol key stream to the remote location* (see column 3, lines 19-24 and column 4, lines 47-49); **Long et al** also discloses the voice packets having a clock counter to synchronize cryptographic operations between encryption equipments 10 and 20 (column 3, lines 19-23) that meets the recitation of *wherein the voice packets having a timestamp as a synchronization source operable to synchronize cryptographic operations between said local and remote locations.*

Long et al is silent about the data being voice data and collision detection. It is apparent to one of ordinary skill in the art that the invention may be applied to any type of data communication as known in the art including radio communication using voice packets. **Dent** in an analogous art also discloses synchronization using real-time clock and counters operable to synchronize cryptographic operations between a transmitter and a receiver in cellular radio system using voice packets (see column 12, line 23 through column 13, line 10). The equipment may be used for secure communication over digital channel for converting a voice signal into digital signal (see column 8, lines 54-66). Dent discloses a collision is detected wherein the multimedia terminal adapters have the same source identifier (see column 14, lines 21-49) and further discloses generating a second steam in response to handoff as discussed above with respect to claim 1 (see also column 15, lines 30-44). Dent illustrates detecting a collision and restarting a new session (see column 12, line 23 through column 13, line 16, the failure of synchronization is due to a collision as understood by Examiner). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the system of **Long et al** into cellular radio communications so as to securely transmit voice packets using

synchronization technique and convert voice packet to digital data stream and vice versa as suggested by **Dent** above.

Although the term “gateway” is not explicitly cited in **Long et al**, it could be interpreted as a software, which meets the claimed limitation. In addition, Examiner takes official notice that gateway is notoriously well known in network communication for forwarding data and performing network protocol conversion. The use of gateway is explicitly cited in Crichton and in RFC 2833 for forwarding encrypted data. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a gateway for receiving and forwarding data because if it is implemented as a hardware, it would allow control of traffic before the data actually reaches the equipments 10 and 20 and would provide load balancing.

Claim 18 is similar to the rejected **claim 15**, except for adding a synchronization source identifier, which is known in the art as found in US patents 6,2754,71 and 6,122,665. **Long et al.** also uses a key identifier that meets the recitation of synchronization source identifier, for example (see **Long et al**, column 3, lines 5-23).

Allowable Subject Matter

7. Claims 6 and 10-12 are allowed.

7.1 Claims 2 and 10 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARL COLIN whose telephone number is (571)272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

Art Unit: 2433

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Primary Examiner, Art Unit 2433
July 7, 2009